PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-288321
(43)Date of publication of application : 10.10.2003

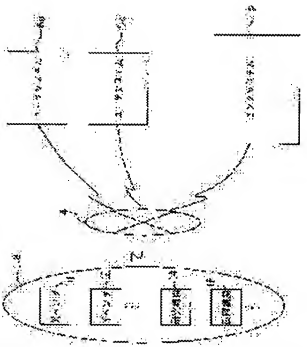
(51)Int.Cl. G06F 15/00
G06F 17/30

(21)Application number : 2002-090840
(22)Date of filing : 28.03.2002

(71)Applicant : NRI & NCC CO LTD
(72)Inventor : TERADA HIROSHI
MASHITA TATSUMI

(54) SECURITY INFORMATION MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a security information management system capable of surely providing a user system with necessary security information.
SOLUTION: In user systems 6a and 6b, information on basic software, etc., used in the user systems is previously registered in the user systems as setting information while it is transmitted to a center system 2. The center system 2 receives and stores therein the transmitted setting information. The center system 2 collects security information disclosed to the public via the Internet 4 by a security information supply source 8, selects security information needed by the respective user systems based on the previously stored setting information, and transmits the selected security information to the respective user systems.



LEGAL STATUS

[Date of request for examination] 24.03.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－288321
（P2003－288321A）
(43)公開日　平成15年10月10日(2003.10.10)

(51)Int.Cl.[7]		識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ａ　５Ｂ０７５
	17/30	１７０		17/30	１７０Ｚ　５Ｂ０８５

審査請求　有　請求項の数６　ＯＬ　（全 10 頁）

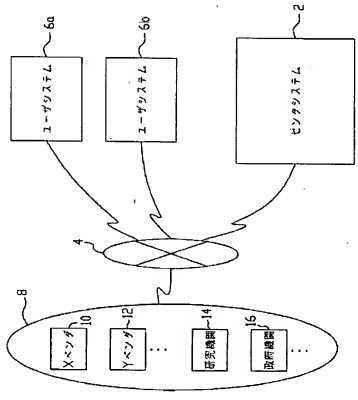
(21)出願番号　特願2002－90840(P2002－90840)
(22)出願日　平成14年３月28日(2002.3.28)

(71)出願人　000155469
株式会社野村総合研究所
東京都千代田区大手町二丁目２番１号
(72)発明者　寺田　洋
東京都千代田区大手町１－６－１　エヌ・アール・アイ・セキュア・テクノロジーズ株式会社内
(74)代理人　100112427
弁理士　藤本　芳洋　（外２名）

最終頁に続く

(54)【発明の名称】　セキュリティ情報管理システム

(57)【要約】
【課題】　必要なセキュリティ情報をユーザシステムに的確に提供することができるセキュリティ情報管理システムを提供する。
【解決手段】　ユーザシステム６ａ、６ｂにおいては、各ユーザシステム内において使用されている基本ソフトウェア等に関する情報を設定情報として予めユーザシステム内で登録すると共に、センタシステム２に対して送信する。センタシステム２においては、送信された設定情報を受信して記憶する。また、センタシステム２においてセキュリティ情報提供元８によりインターネット４を介して公開されているセキュリティ情報を収集し、予め記憶されている設定情報に基づいて各ユーザシステムにおいて必要なセキュリティ情報を選択し、選択したセキュリティ情報を各ユーザシステムに対して送信する。



1

【特許請求の範囲】

【請求項１】　マスタサーバを備えるセンタシステムと、エージェントサーバを備えるユーザシステムとが、ネットワークを介して相互に接続されているセキュリティ情報管理システムにおいて、

前記マスタサーバは、

前記ネットワークにおいて公開されているセキュリティ情報を収集するセキュリティ情報収集手段と、

前記セキュリティ情報を記憶するセキュリティ情報記憶手段と、

前記エージェントサーバから前記ネットワークを介して送信された設定情報を受信する設定情報受信手段と、

前記設定情報を記憶する設定情報記憶手段と、

前記設定情報記憶手段に記憶されている設定情報に基づいて、前記セキュリティ情報記憶手段に記憶されているセキュリティ情報の中から前記エージェントサーバに対して送信するセキュリティ情報を選択するセキュリティ情報選択手段と、

前記セキュリティ情報選択手段により選択されたセキュリティ情報を前記エージェントサーバに対して送信するセキュリティ情報送信手段とを備え、

前記エージェントサーバは、

前記設定情報が登録されている設定情報登録手段と、

前記設定情報を前記マスタサーバに対して送信する設定情報送信手段と、

前記マスタサーバから前記ネットワークを介して送信された前記セキュリティ情報を受信するセキュリティ情報受信手段と、

前記セキュリティ情報をユーザ端末に対して提供するセキュリティ情報提供手段とを備えることを特徴とするセキュリティ情報管理システム。

【請求項２】　マスタサーバを備えるセンタシステムと、エージェントサーバを備える複数のユーザシステムとが、ネットワークを介して相互に接続されているセキュリティ情報管理システムにおいて、

前記エージェントサーバは、

設定情報が登録されている設定情報登録手段と、

前記設定情報を前記マスタサーバに対して送信する設定情報送信手段と、

前記ユーザシステム内において異常が発生したことを検知する異常検知手段と、

前記異常検知手段により検知された異常を異常検知情報として、前記マスタサーバに対して送信する異常検知情報送信手段とを備え、

前記マスタサーバは、

前記複数のユーザシステムの各々が備えるエージェントサーバから前記ネットワークを介して送信された設定情報を受信する設定情報受信手段と、

前記設定情報受信手段により受信された前記ユーザシステム毎の前記設定情報を記憶する設定情報記憶手段と、

2

前記エージェントサーバから送信された異常検知情報を受信する異常検知情報受信手段と、

前記異常検知情報受信手段において、前記異常検知情報を受信した場合に、前記設定情報記憶手段に記憶されている前記ユーザシステム毎の前記設定情報に基づいて、前記異常検知情報に基づく警告情報を送信するエージェントサーバを特定するエージェントサーバ特定手段と、

前記エージェントサーバ特定手段により特定されたエージェントサーバに対して、前記警告情報を送信する警告情報送信手段とを備えることを特徴とするセキュリティ情報管理システム。

【請求項３】　前記エージェントサーバ特定手段は、前記異常検知情報受信手段において、複数の前記エージェントサーバから類似内容の異常検知情報を受信した場合に、前記警告情報を送信するエージェントサーバを特定することを特徴とする請求項２記載のセキュリティ情報管理システム。

【請求項４】　前記マスタサーバは、

前記ネットワークにおいて公開されているセキュリティ情報を収集するセキュリティ情報収集手段と、

前記セキュリティ情報を記憶するセキュリティ情報記憶手段と、

前記設定情報記憶手段に記憶されている前記ユーザシステム毎の前記設定情報に基づいて、前記セキュリティ情報記憶手段に記憶されているセキュリティ情報の中から前記エージェントサーバに対して送信するセキュリティ情報を選択するセキュリティ情報選択手段と、

前記セキュリティ情報選択手段により選択されたセキュリティ情報を前記エージェントサーバに対して送信するセキュリティ情報送信手段とを更に備え、

前記エージェントサーバは、

前記セキュリティ情報を受信するセキュリティ情報受信手段と、

前記セキュリティ情報を記憶するセキュリティ情報記憶手段と、

前記警告情報受信手段により警告情報を受信した場合又は前記異常検知手段により異常を検知した場合に、前記セキュリティ情報記憶手段に記憶されているセキュリティ情報の中に、前記警告情報に基づく警告への対応策に関する情報又は前記異常に対する対応策に関する情報が存在しているか否かを検索する対応策検索手段と、

前記対応策検索手段により対応策に関する情報が検索された場合に、前記対応策に関する情報をユーザ端末に対して提供する対応策提供手段とを更に備えることを特徴とする請求項２又は請求項３記載のセキュリティ情報管理システム。

【請求項５】　前記設定情報は、前記ユーザシステムにおいて使用されている基本ソフトウェアの種類、前記基本ソフトウェアのバージョン、閲覧用ソフトウェアの種類、前記閲覧用ソフトウェアのバージョン、コンピュー

タウィルス検知駆除ソフトウェアの種類、前記コンピュータウィルス検知駆除ソフトウェアのバージョン及びそのウィルスパターンファイルのバージョンの情報の中の少なくとも一つを含むことを特徴とする請求項１～請求項４の何れか一項に記載のセキュリティ情報管理システム。

【請求項６】　前記エージェントサーバは、前記ユーザシステム内において所定の検知プログラムを作動させることによって、前記設定情報とすべき前記ユーザシステムに関する詳細情報を収集する詳細情報収集手段と、前記詳細情報収集手段により収集された詳細情報を登録する詳細情報登録手段とを更に備えることを特徴とする請求項１～請求項５の何れか一項に記載のセキュリティ情報管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コンピュータセキュリティに関するセキュリティ情報の管理を行うセキュリティ情報管理システムに関するものである。

【０００２】

【従来の技術】従来、コンピュータセキュリティに関する情報（セキュリティ情報）は、ソフトウェア製品等を扱っている企業、販売店（ベンダ）あるいは研究機関等によりインターネットを介して公開されている。そのため、ユーザシステムの管理を行っているシステム管理者等は、インターネットを介して公開されている情報の中から自らが管理しているユーザシステムに必要な情報を選別し、必要な情報の収集を行っていた。

【０００３】

【発明が解決しようとする課題】ところで、ベンダや研究機関等の多くの情報提供元は、頻繁に新しいセキュリティ情報をインターネットを介して公開しており、システム管理者等が公開されている全ての情報をチェックすることは困難である。また、インターネットを介して公開されているセキュリティ情報の中には、様々な基本ソフトウェア、閲覧用ソフトウェア等に関するセキュリティ情報が含まれている。そのため、システム管理者は、管理を行っているユーザシステムにおいて使用されているソフトウェアのバージョンの情報等を調査した上で、それらに必要なセキュリティ情報等を探し出して収集しなければならず、必要なセキュリティ情報を得るために多くの手間が必要となっている。

【０００４】この発明の課題は、必要なセキュリティ情報をユーザシステムに的確に提供することができるセキュリティ情報管理システムを提供することである。

【０００５】

【課題を解決するための手段】請求項１記載のセキュリティ情報管理システムは、マスタサーバを備えるセンタシステムと、エージェントサーバを備えるユーザシステムとが、ネットワークを介して相互に接続されているセキュリティ情報管理システムにおいて、前記マスタサーバは、前記ネットワークにおいて公開されているセキュリティ情報を収集するセキュリティ情報収集手段と、前記セキュリティ情報を記憶するセキュリティ情報記憶手段と、前記エージェントサーバから前記ネットワークを介して送信された設定情報を受信する設定情報受信手段と、前記設定情報を記憶する設定情報記憶手段と、前記設定情報記憶手段に記憶されている設定情報に基づいて、前記セキュリティ情報記憶手段に記憶されているセキュリティ情報の中から前記エージェントサーバに対して送信するセキュリティ情報を選択するセキュリティ情報選択手段と、前記セキュリティ情報選択手段により選択されたセキュリティ情報を前記エージェントサーバに対して送信するセキュリティ情報送信手段とを備え、前記エージェントサーバは、前記設定情報が登録されている設定情報登録手段と、前記設定情報を前記マスタサーバに対して送信する設定情報送信手段と、前記マスタサーバから前記ネットワークを介して送信された前記セキュリティ情報を受信するセキュリティ情報受信手段と、前記セキュリティ情報をユーザ端末に対して提供するセキュリティ情報提供手段とを備えることを特徴とする。

【０００６】この請求項１記載のセキュリティ情報管理システムによれば、マスタサーバにおいて収集されたセキュリティ情報を、エージェントサーバから送信され、予め受信・記憶されている設定情報に基づいて選択した後に、エージェントサーバに対して送信している。そして、エージェントサーバを介してユーザ端末にセキュリティ情報が提供されている。従って、例えば、ユーザシステムにおいて使用している基本ソフトウェアの種類等に基づいて、ユーザシステムにおいて必要なセキュリティ情報をの確に提供することができる。

【０００７】また、請求項２記載のセキュリティ情報管理システムは、マスタサーバを備えるセンタシステムと、エージェントサーバを備える複数のユーザシステムとが、ネットワークを介して相互に接続されているセキュリティ情報管理システムにおいて、前記エージェントサーバは、設定情報が登録されている設定情報登録手段と、前記設定情報を前記マスタサーバに対して送信する設定情報送信手段と、前記ユーザシステム内において異常が発生したことを検知する異常検知手段と、前記異常検知手段により検知された異常を異常検知情報として、前記マスタサーバに対して送信する異常検知情報送信手段とを備え、前記マスタサーバは、前記複数のユーザシステムの各々が備えるエージェントサーバから前記ネットワークを介して送信された設定情報を受信する設定情報受信手段と、前記設定情報受信手段により受信された前記ユーザシステム毎の前記設定情報を記憶する設定情報記憶手段と、前記エージェントサーバから送信された異常検知情報を受信する異常検知情報受信手段と、前記異常検知情報受信手段において、前記異常検知情報を受

信した場合に、前記設定情報記憶手段に記憶されている前記ユーザシステム毎の前記設定情報に基づいて、前記異常検知情報に基づく警告情報を送信するエージェントサーバを特定するエージェントサーバ特定手段と、前記エージェントサーバ特定手段により特定されたエージェントサーバに対して、前記警告情報を送信する警告情報送信手段とを備えることを特徴とする。

【０００８】この請求項２記載のセキュリティ情報管理システムによれば、複数のユーザシステムの各々が備えるエージェントサーバが、ユーザシステム内において異常が発生したか否かを検知し、異常を検知した場合にはマスタサーバに対して異常検知情報を送信している。そして、異常検知情報を受信したマスタサーバにおいては、予め設定されているユーザシステム毎の設定情報に基づいて異常が発生したユーザシステムと同一のソフトウェアを使用している等の他のユーザシステムに対して警告情報を送信している。従って、あるユーザシステムにおいて異常が発生した場合には、同様の異常が発生する可能性がある他のユーザシステムに対して異常が発生する可能性があることを迅速に警告することができる。

【０００９】また、請求項３記載のセキュリティ情報管理システムは、前記エージェントサーバ特定手段が、前記異常検知情報受信手段において、複数の前記エージェントサーバから類似内容の異常検知情報を受信した場合に、前記警告情報を送信するエージェントサーバを特定することを特徴とする。

【００１０】この請求項３記載のセキュリティ情報管理システムによれば、複数のエージェントサーバから類似内容の異常検知情報を受信した場合、例えば、複数のエージェントサーバから同一のソフトウェアに関する異常検知情報を受信した等の場合には、そのソフトウェアを使用している他のエージェントサーバに対して警告情報を送信している。従って、特定のソフトウェアについて異常が発生する可能性が高いことを高精度に警告することができる。

【００１１】また、請求項４記載のセキュリティ情報管理システムは、前記マスタサーバが、前記ネットワークにおいて公開されているセキュリティ情報を収集するセキュリティ情報収集手段と、前記セキュリティ情報を記憶するセキュリティ情報記憶手段と、前記設定情報記憶手段に記憶されている前記ユーザシステム毎の前記設定情報に基づいて、前記セキュリティ情報記憶手段に記憶されているセキュリティ情報の中から前記エージェントサーバに対して送信するセキュリティ情報を選択するセキュリティ情報選択手段と、前記セキュリティ情報選択手段により選択されたセキュリティ情報を前記エージェントサーバに対して送信するセキュリティ情報送信手段とを更に備え、前記エージェントサーバは、前記セキュリティ情報を受信するセキュリティ情報受信手段と、前記セキュリティ情報を記憶するセキュリティ情報記憶手段と、前記警告情報受信手段により警告情報を受信した場合又は前記異常検知手段により異常を検知した場合に、前記セキュリティ情報記憶手段に記憶されているセキュリティ情報の中に、前記警告情報に基づく警告への対応策に関する情報又は前記異常に対する対応策に関する情報が存在しているか否かを検索する対応策検索手段と、前記対応策検索手段により対応策に関する情報が検索された場合に、前記対応策に関する情報をユーザ端末に対して提供する対応策提供手段とを更に備えることを特徴とする。

【００１２】この請求項４記載のセキュリティ情報管理システムによれば、異常を検知した場合又は警告情報を受信した場合には、記憶されているセキュリティ情報の中に対応策に関する情報が存在するか否かの検索を行い、対応策に関する情報が検索された場合には、ユーザ端末に対して対応策に関する情報を提供している。従って、検知された異常又は警告情報に対する対応策に関する情報をユーザ端末に対して迅速に提供することができる。

【００１３】また、請求項５記載のセキュリティ情報管理システムは、前記設定情報が、前記ユーザシステムにおいて使用されている基本ソフトウェアの種類、前記基本ソフトウェアのバージョン、閲覧用ソフトウェアの種類、前記閲覧用ソフトウェアのバージョン、コンピュータウイルス検知駆除ソフトウェアの種類、前記コンピュータウイルス検知駆除ソフトウェアのバージョン及びそのウィルスパターンファイルのバージョンの情報の中の少なくとも一つを含むことを特徴とする。

【００１４】この請求項５記載のセキュリティ情報管理システムによれば、設定情報として基本ソフトウェアの種類、基本ソフトウェアのバージョン等が予め設定されているため、ユーザシステムにおいて必要なセキュリティ情報を的確に提供することができる。

【００１５】また、請求項６記載のセキュリティ情報管理システムは、前記エージェントサーバが、前記ユーザシステム内において所定の検知プログラムを作動させることによって、前記設定情報とすべき前記ユーザシステムに関する詳細情報を収集する詳細情報収集手段と、前記詳細情報収集手段により収集された詳細情報を登録する詳細情報登録手段とを更に備えることを特徴とする。

【００１６】この請求項６記載のセキュリティ情報管理システムによれば、エージェントサーバが設定情報とすべきユーザシステムに関する詳細情報を更に収集し、登録している。従って、例えば、エージェントサーバにおいてユーザシステム内のセキュリティ環境等を詳細に把握することができる。

【００１７】

【発明の実施の形態】以下、図面を参照して、この発明の実施の形態に係るセキュリティ情報管理システムについて説明する。

【００１８】図１は、実施の形態に係るセキュリティ情報管理システムのブロック構成図である。セキュリティ情報管理システムは、図１に示すように、センタシステム２を備え、このセンタシステム２は、インターネット４を介してユーザシステム６ａ、６ｂ及びセキュリティ情報提供元８と接続されている。

【００１９】図２は、センタシステム２に備えられているマスタサーバ２０のブロック構成図である。この図２に示すように、マスタサーバ２０は、セキュリティ情報の収集等の処理を行うデータ処理部２２を備え、このデータ処理部２２には、ユーザシステム６ａ、６ｂ及びセキュリティ情報提供元８との間の通信を制御する通信制御部２４、ユーザシステム毎の設定情報を記憶している設定情報記憶部２６及び収集されたセキュリティ情報等を記憶しているデータ記憶部２８が接続されている。

【００２０】ここで、設定情報記憶部２６に記憶されている設定情報は、各ユーザシステムからインターネット４を介して予め送信されている情報である。即ち、各ユーザシステムにおいて登録された設定情報は、ユーザシステム内において、後述の設定情報登録部４６（図３参照）に記憶されると共に、マスタサーバ２０に対して送信される。そして、マスタサーバ２０においては、各ユーザシステムから送信された設定情報を通信制御部２４を介して受信し、各ユーザシステム毎に設定情報記憶部２６に記憶する。なお、この設定情報は、各ユーザシステム毎に必要なセキュリティ情報を選択する際に用いる情報であり、ユーザシステム毎に付与されているユーザシステムＩＤに対応させて記憶されている。

【００２１】図３は、ユーザシステム６ａのブロック構成図である。この図３に示すように、ユーザシステム６ａは、エージェントサーバ４０及びユーザ端末５０ａ、５０ｂを備え、エージェントサーバ４０とユーザ端末５０ａ、５０ｂとは通信ネットワークを介して相互に接続されている。なお、ユーザシステム６ｂは、ユーザシステム６ａと同様の構成であるため説明を省略する。

【００２２】エージェントサーバ４０は、ユーザ端末５０ａ、５０ｂに対してセキュリティ情報の提供等の処理を行うデータ処理部４２を備え、このデータ処理部４２には、マスタサーバ２０及びユーザ端末５０ａ、５０ｂとの間の通信を制御する通信制御部４４が接続されている。また、データ処理部４２には、ユーザシステム６ａを管理しているシステム管理者等により登録された設定情報が登録されている設定情報登録部４６、セキュリティ情報等を記憶するデータ記憶部４８が接続されている。

【００２３】ここで、設定情報登録部４６に登録されている設定情報には、ユーザシステム６ａにおいて使用されている基本ソフトウェアの種類、基本ソフトウェアのバージョン、閲覧用ソフトウェアの種類及び閲覧用ソフトウェアのバージョン等の情報及び、システム管理者等が提供を希望しているセキュリティ情報を指定したセキュリティ情報指定情報が含まれている。なお、セキュリティ情報指定情報とは、例えば、ユーザシステム６ａが使用している外部データベースやプロバイダに関する情報等、セキュリティ情報として提供される内容を指定する情報である。

【００２４】また、エージェントサーバ４０の設定情報登録部４６には、システム管理者により設定された設定情報に加えて、ユーザ端末５０ａ、５０ｂに関する詳細情報が記憶されている。即ち、エージェントサーバ４０は、ユーザシステム６ａ内に設置されているユーザ端末５０ａ、５０ｂ内で所定の検知プログラムを作動させる。この検知プログラムを作動させることにより、ユーザ端末５０ａ、５０ｂ内で使用されているソフトウェアのバージョンの細目等、ユーザ端末に関する詳細な情報を収集する。そして、収集された情報を詳細情報としてユーザ端末毎に付与されているユーザ端末ＩＤに対応させて設定情報登録部４６に記憶している。なお、ユーザシステム６ｂ内に設置されているエージェントサーバは、エージェントサーバ４０と同様の構成であるため説明を省略する。

【００２５】また、ユーザ端末５０ａは、データ処理部５２を備え、このデータ処理部５２には、エージェントサーバ４０との間の通信を制御する通信制御部５４、セキュリティ情報等を記憶するデータ記憶部５６及びセキュリティ情報等を表示する表示部５８が接続されている。なお、ユーザ端末５０ｂは、ユーザ端末５０ａと同様の構成であるため説明を省略する。

【００２６】また、セキュリティ情報提供元８には、図１に示すように、コンピュータソフトウェアの販売等を行っているＸベンダ１０、Ｙベンダ１２、コンピュータセキュリティに関する研究等を行っている研究機関１４及びコンピュータセキュリティに関する各種の情報の提供等を行っている政府機関１６等のシステムが含まれる。

【００２７】次に、図４に示すフローチャートを参照して、セキュリティ情報管理システムにおけるセキュリティ情報管理処理について説明する。

【００２８】まず、マスタサーバ２０は、セキュリティ情報提供元８によりインターネット４を介して公開されている情報を収集し（ステップＳ１０）、データ記憶部２８に記憶する（ステップＳ１１）。即ち、Ｘベンダ１０等のソフトウェア販売会社により、インターネット４を介して公開されている各種ソフトウェアに関するコンピュータウィルスについての情報、研究機関１４及び政府機関１６により報告されているシステムの攻撃されやすさ（外部から侵入される可能性）等のシステムの脆弱性に関する情報等を収集し、収集した情報をセキュリティ情報としてデータ記憶部２８に記憶する。

【００２９】次に、各ユーザシステムにおいて必要なセ

キュリティ情報を選択する（ステップＳ１２）。即ち、予め設定情報記憶部２６に記憶されている設定情報を参照し、データ記憶部２８に記憶されているセキュリティ情報の中から各ユーザシステムにおいて必要なセキュリティ情報を選択する。例えば、まず、ユーザシステム６ａの設定情報を参照し、データ記憶部２８に記憶されているセキュリティ情報の中からユーザシステム６ａ内において使用されている基本ソフトウェア等に関係するセキュリティ情報を選択する。次に、ユーザシステム６ｂの設定情報を参照し、ユーザシステム６ｂに必要なセキュリティ情報の選択を行う。同様に、他のユーザシステムの設定情報を参照して、他のユーザシステムに必要なセキュリティ情報の選択を行う。なお、データ記憶部２８に記憶されているセキュリティ情報に対応する基本ソフトウェアや閲覧用ソフトウェアを使用しているユーザシステムが存在しない場合には、処理を終了する。

【００３０】設定情報記憶部２６に記憶されている全てのユーザシステムの設定情報を参照し、各ユーザシステムにおいて必要なセキュリティ情報が選択された場合には（ステップＳ１３）、選択されたセキュリティ情報を各ユーザシステム内に設置されているエージェントサーバに対して送信する（ステップＳ１４）。例えば、ユーザシステム６ａにおいて必要なセキュリティ情報はエージェントサーバ４０に、ユーザシステム６ｂにおいて必要なセキュリティ情報はユーザシステム６ｂのエージェントサーバに対して送信する。また、その他のユーザシステムにおいて必要なセキュリティ情報も、各ユーザシステムのエージェントサーバに対して送信する。

【００３１】ここで、エージェントサーバ４０においては、通信制御部４４を介してセキュリティ情報を受信し、受信したセキュリティ情報をデータ記憶部４８に記憶すると共に、ユーザ端末５０ａ、５０ｂに対して送信する。そして、例えば、ユーザ端末５０ａにおいては、通信制御部５４を介してセキュリティ情報を受信し、受信したセキュリティ情報をデータ記憶部５６に記憶すると共に、表示部５８に表示する。

【００３２】この実施の形態に係るセキュリティ情報管理システムによれば、マスタサーバから、予め記憶されている設定情報に基づいて必要なセキュリティ情報がエージェントサーバに対して送信されている。従って、ユーザシステムにおいては、必要なセキュリティ情報のみの提供を受けることができ、膨大なセキュリティ情報の中から必要なセキュリティ情報を選択する手間を大幅に削減することができる。

【００３３】また、ユーザシステムにおいては、設定情報に基づいて必要なセキュリティ情報を受信することができるため、必要な情報の収集漏れ等がなく、確実に必要なセキュリティ情報を得ることができる。

【００３４】なお、上述の実施の形態においては、マスタサーバから送信されたセキュリティ情報を各ユーザシステム内のエージェントサーバを介して各ユーザ端末に提供しているが、エージェントサーバからシステム管理者が使用しているユーザ端末（管理者用ユーザ端末）を介して各ユーザ端末にセキュリティ情報を提供するようにしてもよい。即ち、エージェントサーバにおいて受信されたセキュリティ情報を、管理者用ユーザ端末に送信し、システム管理者が各ユーザ端末に送信する必要があるセキュリティ情報を選別した後に、選別されたセキュリティ情報を各ユーザ端末に対して送信するようにしてもよい。

【００３５】次に、図１～図３のブロック構成図及び、図５及び図６のフローチャートを参照して、この実施の形態に係るセキュリティ情報管理システムによる他のセキュリティ情報管理処理について説明する。

【００３６】まず、図５のフローチャートを参照して、エージェントサーバにおける処理について説明する。なお、以下においては、ユーザシステム６ａのエージェントサーバ４０における処理を例として説明する。

【００３７】まず、ユーザシステム６ａ内において異常が発生したことを検知したか否かの判断を行う（ステップＳ２０）。即ち、ユーザシステム６ａを監視し、急激に通信量が増加した等の異常が発生したか否かの判断を行う。

【００３８】ユーザシステム６ａ内において異常が発生したことを検知した場合には（ステップＳ２０）、マスタサーバ２０に対して異常が発生したこと及び発生した異常の内容を通報するための異常検知情報を作成する（ステップＳ２１）。例えば、急激に通信量が増加する異常が発生し、この異常はユーザ端末から特定の閲覧用ソフトウェアを用いて特定のホームページに接続した際にウイルスに感染したために発生した可能性が高い等の異常検知情報を作成する。

【００３９】次に、ステップＳ２１において作成した異常検知情報を、通信制御部４４を介してマスタサーバ２０に送信する（ステップＳ２２）。なお、異常検知情報には、エージェントサーバ４０が設置されているユーザシステム６ａのユーザシステムＩＤが付されている。

【００４０】次に、ステップＳ２０において検知された異常に対する対応策に関する情報の検索を行う（ステップＳ２３）。即ち、データ記憶部４８に記憶されているセキュリティ情報の中に、ステップＳ２０において検知した異常に対する対応策に関する情報、例えば、閲覧用ソフトウェアのバージョンアップにより対応することができる等の情報が存在するか否かの検索を行う。

【００４１】データ記憶部４８に記憶されているセキュリティ情報を検索した結果、対応策に関する情報が検索された場合には（ステップＳ２４）、検索された対応策に関する情報をユーザシステム６ａ内のユーザ端末５０ａ、５０ｂに対して提供する（ステップＳ２５）。例えば、閲覧用ソフトウェアをバージョンアップすることに

より発生した異常を解消することができること及びバージョンアップ版の閲覧用ソフトウェアをダウンロードすることができるＵＲＬ（Uniform Resource Locator）の情報等をユーザ端末５０ａ、５０ｂに対して送信する。

【００４２】次に、図６のフローチャートを参照して、異常検知情報を受信したマスタサーバにおける処理を説明する。なお、以下においては、特定の閲覧用ソフトウェアに関する異常検知情報を受信した場合を例として説明する。

【００４３】まず、ユーザシステム６ａのエージェントサーバ４０から送信された異常検知情報を、通信制御部２４を介して受信し（ステップＳ３０）、受信した異常検知情報をデータ記憶部２８に記憶する（ステップＳ３１）。なお、受信した異常検知情報は、発生した異常の内容を確認した後に、異常検知情報に付されているユーザシステムＩＤに対応させてデータ記憶部２８に記憶される。

【００４４】所定の時間内に少なくとも２以上のエージェントサーバから類似内容の異常検知情報を受信したか否かの判断を行う（ステップＳ３２）。即ち、所定の時間内に１のエージェントサーバからのみ異常検知情報が送信された場合には、そのエージェントサーバが設置されているユーザシステム固有の異常が発生又は、異常が発生したかのような処理が行われた可能性がある。一方、所定の時間内、例えば、５分以内等に、複数のエージェントサーバから類似内容の異常検知情報を受信した場合には、使用している特定の閲覧用ソフトウェア等に基づく異常が発生した可能性が高い。そのため、所定の時間内に少なくとも２以上のエージェントサーバから類似内容の異常検知情報を受信したか否かを判断する。

【００４５】所定の時間内に少なくとも２以上のエージェントサーバから類似内容の異常検知情報を受信した場合には（ステップＳ３２）、設定情報記憶部２６に記憶されている設定情報に基づいて、特定の閲覧用ソフトウェアを使用しているユーザシステムを検索する（ステップＳ３３）。即ち、各ユーザシステム毎の設定情報に基づいて、異常が発生したユーザシステムと同じ閲覧用ソフトウェアを使用している他のユーザシステムを検索する。

【００４６】設定情報記憶部２６に記憶されている全てのユーザシステムの設定情報を検索し（ステップＳ３４）、異常が発生したユーザシステムと同一の閲覧用ソフトウェアを使用している他のユーザシステムが検索された場合には（ステップＳ３５）、検索されたユーザシステムに対して警告情報を送信する（ステップＳ３６）。即ち、発生した異常の内容、例えば、特定の閲覧用ソフトウェアを用いて特定のホームページに接続した場合にウィルスに感染する可能性が高い等の警告情報を送信する。

【００４７】ここで、警告情報を受信したエージェントサーバにおいては、ユーザシステム内のユーザ端末に対して警告情報を送信すると共に、図５のフローチャートのステップＳ２３～ステップＳ２５の処理と同様の処理を行う。即ち、警告情報により警告された異常に対する対応策に関する情報がデータ記憶部の中に存在するか否かの検索を行い（ステップＳ２３）、対応策に関する情報が存在する場合には（ステップＳ２４）、各ユーザ端末に対して警告情報と併せて対応策に関する情報を提供する（ステップＳ２５）。

【００４８】この実施の形態のセキュリティ情報管理システムによれば、複数のエージェントサーバから類似内容の異常検知情報が送信された場合には、異常が発生したユーザシステムと同一の閲覧用ソフトウェア等を使用している他のユーザシステムに対して警告情報を送信している。従って、ユーザシステムにおいては、異常が発生する確率が高いソフトウェア等についての警告情報を受信することにより、予め所定の対応をとることができ、ユーザシステム内のセキュリティレベルを高く保つことができる。

【００４９】また、異常を検知したエージェントサーバ及び警告情報を受信したエージェントサーバにおいて、検知された異常又は警告情報に対する対応策に関する情報が存在する場合には、対応策に関する情報を各ユーザ端末に対して提供しているため、発生した異常に対する迅速な対応又は警告情報に基づいて異常に対する的確な予防を施すことができる。

【００５０】なお、上述の実施の形態に係るセキュリティ情報管理システムにおいては、エージェントサーバから対応策に関する情報を提供しているが、マスタサーバにおいて警告情報に対する対応策に関する情報が存在する場合には、警告情報と併せて対応策に関する情報を送信するようにしてもよい。即ち、マスタサーバにおいて収集されているセキュリティ情報の検索を行い、受信した異常検知情報に対する対応策に関する情報が存在する場合には、その対応策に関する情報を警告情報と併せて送信するようにしてもよい。また、異常検知情報に対する対応策に関する情報が存在する場合には、異常検知情報の送信元であるエージェントサーバに対しても対応策に関する情報を送信するようにしてもよい。

【００５１】また、各ユーザシステムのエージェントサーバにおいて、対応策に関する情報を提供した後に所定の時間内にユーザ端末内において対応策が実行されたか否かを監視するようにしてもよい。例えば、ユーザ端末内で検知プログラムを作動させることにより、閲覧用ソフトウェアのバージョンアップが行われたか否かの監視を行い、バージョンアップが行われていない場合には、至急バージョンアップを行うように警告する等メッセージ等を送信するようにしてもよい。

【００５２】

【発明の効果】この発明によれば、マスタサーバにおい

て収集されたセキュリティ情報を、エージェントサーバから送信され、予め受信・記憶されている設定情報に基づいて選択した後に、エージェントサーバに対して送信している。そして、エージェントサーバを介してユーザシステム内の各ユーザ端末にセキュリティ情報が提供されている。従って、例えば、ユーザシステムにおいて使用している基本ソフトウェアの種類等に基づいて、ユーザシステムにおいて必要なセキュリティ情報を的確に提供することができる。そのため、膨大な量のセキュリティ情報の中から必要なセキュリティ情報を選別して収集するための労力を大幅に削減することができる。

【００５３】また、ユーザシステムにおいては、予めユーザシステムにおいて使用されている基本ソフトウェア等に関する情報を設定情報として登録することにより、ユーザシステムにおいて必要なセキュリティ情報の収集漏れ等がなく、確実に必要なセキュリティ情報を得ることができる。

【００５４】また、複数のユーザシステムの各々が備えるエージェントサーバが、ユーザシステム内において異常が発生したか否かを検知し、異常を検知した場合にはマスタサーバに対して異常を通報している。そして、マスタサーバにおいては、異常検知情報を受信した場合には、予め設定されているユーザシステム毎の設定情報に基づいて異常が発生したユーザシステムと同一のソフトウェアを使用している等の他のユーザシステムに対して警告情報を送信している。従って、あるユーザシステムにおいて異常が発生した場合には、同様の異常が発生する可能性がある他のユーザシステムに対して異常が発生する可能性があることを迅速に警告することができる。

そのため、警告情報を受信したユーザシステムにおいては、例えば、ソフトウェアのバージョンアップを行う等、異常が発生することを回避するために必要な処置を施し、ユーザシステムのセキュリティレベルを高く保つことができる。

【図面の簡単な説明】

【図１】この発明の実施の形態に係るセキュリティ情報管理システムのブロック構成図である。

【図２】この発明の実施の形態に係るセンタシステムに備えられているマスタサーバのブロック構成図である。

【図３】この発明の実施の形態に係るユーザシステムのブロック構成図である。

【図４】この発明の実施の形態に係るセキュリティ情報管理処理を説明するためのフローチャートである。

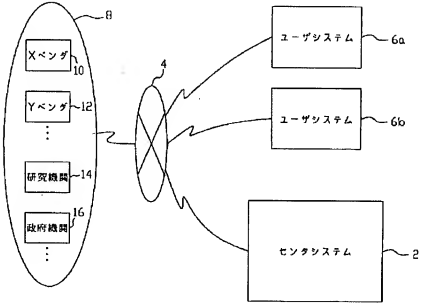
【図５】この発明の実施の形態に係る他のセキュリティ情報管理処理を説明するためのフローチャートである。

【図６】この発明の実施の形態に係る他のセキュリティ情報管理処理を説明するための別のフローチャートである。

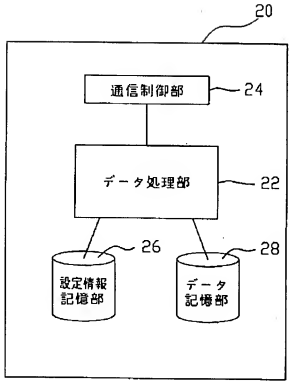
【符号の説明】

２…センタシステム、４…インターネット、６ａ、６ｂ…ユーザシステム、８…セキュリティ情報提供元、２０…マスタサーバ、２２…データ処理部、２４…通信制御部、２６…設定情報記憶部、２８…データ記憶部、４０…エージェントサーバ、４２…データ処理部、部４４…通信制御部、４６…設定情報登録部、４８…データ記憶部、５０ａ、５０ｂ…ユーザ端末、５２…データ処理部、５４…通信制御部、５６…データ記憶部、５８…表示部

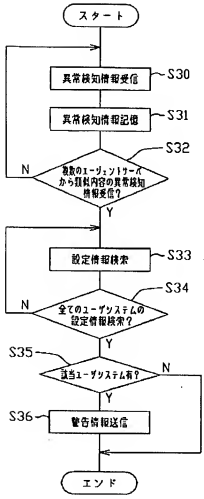
【図１】



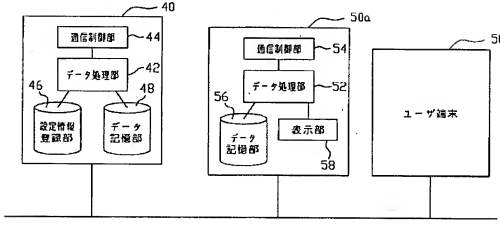
【図２】


20
通信制御部
24
データ処理部
22
26
28
設定情報記憶部
データ記憶部

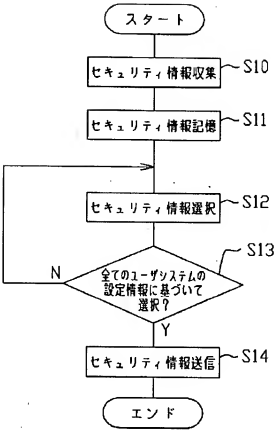
【図６】


スタート
異常検知情報受信
S30
異常検知情報記憶
S31
S32
複数のユーザシステムから類似内容の異常検知情報受信?
N
Y
設定情報検索
S33
S34
全てのユーザシステムの設定情報検索?
N
Y
S35
該当ユーザシステム有?
N
Y
S36
警告情報送信
エンド

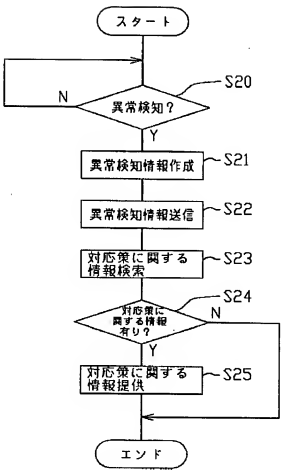
【図３】


40
通信制御部
44
データ処理部
42
46
48
設定情報登録部
データ記憶部
50a
通信制御部
54
データ処理部
52
56
データ記憶部
表示部
58
50b
ユーザ端末

【図４】



【図５】



フロントページの続き

(72)発明者　真下　竜実
東京都千代田区大手町１－６－１　エヌ・アール・アイ・セキュア・テクノロジーズ株式会社内

Ｆターム(参考)　5B075 ND02
5B085 AA01 AA08 AE06 BA07 BG03 BG07